Configuring PPP Services

Router Software Version 10.0
Site Manager Software Version 4.0

Software Version BNX 6.0
Site Manager Software Version BNX 6.0

Part No. 112920 Rev. A
January 1996

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. January 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, BCN, BLN, BN, CN, FRE, LN, Optivity, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and AN, ANH, ASN, BaySIS, BayStack, BCNX, BLNX, BNX, EZ Internetwork, EZ LAN, FN, PathMan, PhonePlus, PPX, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: *This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.*

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Audience xi
Software Suites xii
Before You Begin xii
Bay Networks Customer Support xiii
CompuServe xiii
InfoFACTS xiv
World Wide Web xiv
How to Get Help xiv
Ordering Bay Networks Publications xv
Conventions xv
Acronyms xvi

Chapter 1
PPP Overview

Routing over a PPP Link 1-3
Initializing a PPP Interface 1-4
Establishing the PPP Link 1-4
Authenticating the PPP Link: PAP and CHAP 1-7
Password Authentication Protocol 1-7
Challenge Handshake Authentication Protocol 1-7
Establishing Network Connections 1-8
Datagram Encapsulation 1-8
Monitoring the PPP Link 1-9

Chapter 2
Implementation Notes

PPP Data Compression 2-1
PPP Dial Services Support 2-2
Bandwidth-on-Demand 2-2

Dial-on-Demand 2-2
Dial Backup 2-2
PPP Multiline 2-3
PPP Multilink 2-3
Using PPP Multilink 2-4
Compatibility with Previous Versions 2-5
Balancing Traffic Loads 2-5
Configuring Multilink Operation 2-6
Protocol Prioritization 2-6
Differences between Multiline and Multilink 2-7
PPP Synchronous Line Parameters 2-8
PPP Software Incompatibilities 2-9
Configuring IP to Run over PPP Interfaces 2-10
Disabling Network Control Protocols 2-10
Calculating and Viewing Line Statistics 2-11

Chapter 3
Enabling PPP Service

Enabling PPP on an Interface 3-1

Chapter 4
Editing PPP Parameters

Editing PPP Interface Parameters 4-2
PPP Interface Parameter Descriptions 4-5
Editing PPP Line Parameters 4-15
PPP Line Parameter Descriptions 4-18
Deleting PPP 4-30

Appendix A
PPP Parameter Default Settings

Appendix B
PPP Statistics

Index

Figures

Figure 1-1. Point-to-Point Network Connection 1-1
Figure 1-2. PPP Interface Initialization 1-6
Figure 1-3. PPP-Encapsulated Frame 1-8
Figure 1-4. Link Quality Monitoring from Router A's Perspective 1-10
Figure 2-1. Multilink Circuits 2-4
Figure 4-1. Configuration Manager Window 4-2
Figure 4-2. PPP Interface Lists Window 4-3
Figure 4-3. PPP Line Lists Window 4-16

Tables

Table 1-1. Data Link Control Protocol Options 1-2
Table 1-2. Network Control Protocols and Options 1-3
Table 2-1. Comparing Multiline and PPP Multilink 2-7
Table 2-2. PPP Synchronous Line Parameter Values 2-8
Table A-1. Point-to-Point (PPP) Interface Parameters A-1
Table A-2. Point-to-Point (PPP) Line Parameters A-3
Table B-1. PPP Statistics B-1

About This Guide

If you are responsible for configuring and managing Bay Networks™ routers and/or BNX™ switching platforms running over Point-to-Point links, you need to read this guide.

This guide describes Point-to-Point Protocol (PPP) services and provides instructions for using Site Manager to configure PPP parameters for your network.

Refer to this guide for

- An overview of Point-to-Point Protocol services (Chapter 1)
- Information on the Bay Networks implementation of PPP services (Chapter 2)
- Instructions on enabling PPP (Chapter 3)
- Descriptions of PPP parameters and how to edit those parameters (Chapter 4)
- Default parameter settings (Appendix A)
- PPP Statistics (Appendix B)

See *Configuring Routers* or *Configuring Customer Access (BNX Software)*, depending on your platform, for information and instructions about the following topics:

- Initially configuring and saving a WAN interface
- Retrieving a configuration file
- Rebooting the device with a configuration file

Audience

Written for system and network managers, this guide describes how to configure the Bay Networks implementation of PPP interfaces and how to use the Site Manager tool to manage your environment.

Software Suites

Routing and Switching software is available in the following suites.

- The *System Suite* includes IP routing, 802.1 Transparent Bridge, Source Route Bridge, Translation Bridge, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, and basic DLSw.
- The *LAN Suite* includes DECnet Phase 4, AppleTalk Phase 2, OSI, VINES, IPX, and ATM DXI, in addition to the System Suite.
- The *WAN Suite* includes ATM DXI, Frame Relay, LAPB, and X.25, in addition to the System Suite.
- The *Corporate Suite* includes the System, LAN, and WAN suites in their entirety.
- The *ARE ATM Suite* provides RFC 1483 and 1577 compliance, ATM UNI 3.0 signaling, in addition to the LAN Suite.
- The *ARE VNR Corporate Suite* provides ATM Forum LAN Emulation, in addition to the ARE ATM Suite and Corporate Suite.
- The *BNX Suite* includes IP Routing, SNMP Agent, Bay Networks HDLC, PPP, OSPF, EGP, BGP, File-Based Performance Statistics, Frame Relay switching, and Frame Relay billing, and selected components from the Corporate, ARE ATM, and ARE VNR Corporate suites.

Availability of features and functionality described in this guide depends on the suites you are using.

Before You Begin

Before using this guide, you must

- Create and save a configuration file that contains at least one WAN interface
- Retrieve the configuration file in local, remote, or dynamic mode

Refer to *Configuring Routers* or *Configuring Customer Access (BNX Software)*, depending on your platform, for instructions on how to do these functions.

Bay Networks Customer Support

Bay Networks provides live telephone technical support to our distributors, resellers, and service-contracted customers from two U.S. and three international support centers. If you have purchased your Bay Networks product from a distributor or authorized reseller, contact the technical support staff of that distributor or reseller for assistance with installation, configuration, troubleshooting, or integration issues.

Customers also have the option of purchasing direct support from Bay Networks through a variety of service programs. The programs include priority access telephone support, on-site engineering assistance, software subscription, hardware replacement, and other programs designed to protect your investment.

To purchase any of these support programs, including PhonePlus™ for 24-hour telephone technical support, call 1-800-2LANWAN. Outside the U.S. and Canada, call (408) 764-1000. You can also receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your reseller. Bay Networks provides several methods of receiving support and information on a nonpriority basis through the following automated systems.

CompuServe

Bay Networks maintains an active forum on CompuServe. All you need to join us online is a computer, a modem, and a CompuServe account. We also recommend using the CompuServe Information Manager software, available from CompuServe.

The Bay Networks forum contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. Software agents and patches are available, and the message boards are monitored by technical staff and can be a source for problem solving and shared experiences.

Customers and resellers holding Bay Networks service contracts can visit the special libraries to acquire advanced levels of support documentation and software.

To open an account and receive a local dial-up number, call CompuServe at 1-800-524-3388 and ask for Representative No. 591.

- In the United Kingdom, call Freephone 0800-289378.
- In Germany, call 0130-37-32.
- In Europe (except for the United Kingdom and Germany), call (44) 272-760681.
- Outside the U.S., Canada, and Europe, call (614) 529-1349 and ask for Representative No. 591, or consult your listings for an office near you.

Once you are online, you can reach our forum by typing the command GO BAYNETWORKS at any ! prompt.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system contains libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system can return a fax copy to the caller or to a third party within minutes of being accessed.

World Wide Web

The World Wide Web (WWW) is a global information system for file distribution and online document viewing via the Internet. You need a direct connection to the Internet and a Web Browser (such as Mosaic or Netscape).

Bay Networks maintains a WWW Home Page that you can access at http://www.baynetworks.com. One of the menu items on the Home Page is the Customer Support Web Server, which offers technical documents, software agents, and an E-mail capability for communicating with our technical support engineers.

How to Get Help

For additional information or advice, contact the Bay Networks Technical Response Center in your area:

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-966-968
Sydney, Australia	(61) 2-903-5800
Tokyo, Japan	(81) 3-328-005

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers. You may also request a free catalog of Bay Networks Press product publications.

Phone:	1-800-845-9523
FAX - U.S./Canada:	1-800-582-8000
FAX - International:	1-916-939-1010

Conventions

This section describes the conventions used in this guide.

arrow character (➔)	Separates menu and option names in instructions. Example: Protocols➔AppleTalk identifies the AppleTalk option in the Protocols menu.
bold text	Indicates text that you need to enter and command names in text. Example: Use the **dinfo** command.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BNCP	Bridge Network Control Protocol
BNX	Backbone Node Switch
BOFL	Breath of Life (message)
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CMIP	Common Management Information Protocol
CRC	Cyclic Redundancy Check
DNCP	DECnet Phase IV Control Protocol
EGP	Exterior Gateway Protocol
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
HDLC	High-level Data Link Control
HSSI	High-speed serial interface
IP	Internet Protocol
IPCP	IP Control Protocol
IPX	Internet Packet Exchange
IPXCP	IPX Control Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LQM	Link Quality Monitoring
LQR	Link Quality Report
MAC	Media Access Control
MIB	Management Information Base
MTU	Maximum Transmission Unit
NCP	Network Control Protocol
OSI	Open Systems Interconnection
OSINLCP	OSI Network Layer Control Protocol
PAP	Password Authentication Protocol

RFC	Request for Comment
SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
VINES	Virtual Networking System
VNCP	VINES Network Control Protocol
WAN	Wide Area Network
XNS	Xerox Network System
XNSCP	Xerox Network System Control Protocol

Chapter 1
PPP Overview

Point-to-Point Protocol (PPP) is a standard method of routing or bridging datagrams between peer routers or other devices over serial point-to-point links (Figure 1-1).

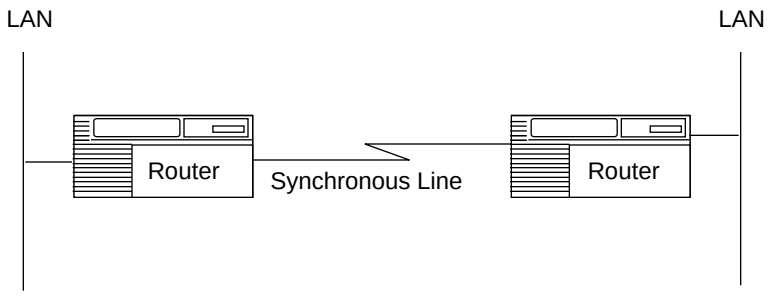


Figure 1-1. Point-to-Point Network Connection

PPP serves three major functions:

- Data link layer connection and management
- Network layer connection and management
- Datagram encapsulation

PPP uses a suite of data link and network control protocols to connect peer routers. PPP also allows peer routers to negotiate and determine data link and network layer options (Table 1-1 and Table 1-2). When negotiations complete successfully, PPP encapsulates the data and transmits it over the link.

Table 1-1. Data Link Control Protocol Options

Option	Function
Maximum Receive Unit	Specifies the Maximum Transmission Unit (MTU) size for the line.
Authentication Protocol: Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP)	Imposes network security by requiring an authentication process.
PAP ID or CHAP Local Name	Text string that identifies the caller for bandwidth-on-demand, dial-on-demand, and dial backup lines.
Link Quality Protocol	Enables or disables link quality monitoring and reporting.
Multilink Endpoint Discriminator	Enables the PPP mulitlink protocol and specifies the identity of the sender of the option.

Table 1-2. Network Control Protocols and Options

Protocol	Negotiable Options
IP Control Protocol (IPCP)	IP Addresses (for backward compatibility), IP Address (default)
Internet Packet Exchange Control Protocol (IPXCP)	IPX Network Number, IPX Node Number, IPX Routing Protocol, IPX Router Name, IPX Configuration Complete
AppleTalk Control Protocol (ATCP)	AppleTalk Network Number, AppleTalk Node Number, AppleTalk Routing Protocol
DECnet Phase IV Control Protocol (DNCP)	None
OSI Network Layer Control Protocol (OSINLCP)	None
Xerox Network System Control Protocol (XNSCP)	None
VINES Network Control Protocol (VNCP)	None
Bridge Network Control Protocol (BNCP)	MAC Type Selection

Routing over a PPP Link

You can enable the following protocols over PPP interfaces:

- AppleTalk
- DECnet Phase IV
- Internet Packet Exchange (IPX)
- Internet Protocol (IP)
- Open Systems Interconnection (OSI)
- Virtual Networking System (VINES)
- Xerox Network System (XNS)

Transparent/Translation Bridge and Source Routing Bridge are other routing media that you can enable over any PPP interface. The PPP bridge accepts incoming traffic from any media (Ethernet, FDDI, Token Ring) and forwards data transparently (or translates when necessary).

Initializing a PPP Interface

PPP creates an interface between peer routers to allow them to exchange data. The routers initialize the interface in three phases:

1. Link establishment
2. Authentication
3. Network layer protocol negotiations

The following sections describe each phase.

Establishing the PPP Link

PPP's Link Control Protocol (LCP) helps establish a link. LCP generates three types of packets:

- Link configuration packets, including Configure-Request, Configure-ACK, Configure-NAK, and Configure-Reject packets
- Link termination packets, including Terminate-Request and Terminate-ACK packets
- Link maintenance packets, including Code-Reject, Protocol-Reject, Echo-Request, and Echo-Reply packets

When two routers initialize a PPP dialogue, each of them sends a Configure-Request packet to the other (peer) router. Each Configure-Request packet contains a list of LCP options and corresponding values that the sending router uses to define its end of the link.

For example, a Configure-Request packet may specify the link's maximum transmission unit (MTU) size and whether the sender wants to use Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The Configure-Request packet contains the user-configured values, which the sender and its peer router may need to negotiate.

Each router receives a Configure-Request packet from its peer. Each router responds with one of three types of packets:

- Configure-ACK

  If a router accepts the proposed LCP options, it responds with a Configure Acknowledgment (ACK) packet.

  When the routers on each side of the link send and receive Configure-ACK packets, the LCP advances to an *open state,* which means that the PPP interface can advance to the next phase.

- Configure-Reject

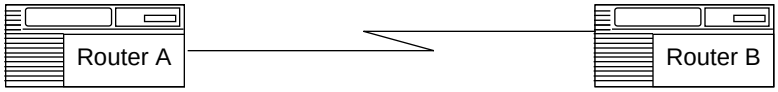
  If the Configure-Request packet contains options that the peer router is not willing to negotiate, the peer router sends back a Configure-Reject packet specifying the nonnegotiable options. From that point on, Configure-Request packets that the originating router sends should no longer specify the unacceptable options.

- Configure-NAK

  If the Configure-Request packet contains proposed values for options that the peer disagrees with, it responds with a Configure Negative Acknowledgment (NAK) packet. The Configure-NAK packet notes the values that the peer disagrees with, and it includes the corresponding values that the peer would like to see in subsequent Configure-Request packets.

LCP negotiations between peers continue until either the routers converge (reach an agreement regarding the Configure-Request) and PPP advances to the next phase or until the peer router transmits a user-specified number of Configure-NAK packets before sending a Configure-Reject packet. When the originating router receives a Configure-Reject packet, the originating router removes the offending options. The routers should then converge.

Figure 1-2 demonstrates how a PPP interface initializes.



1. PPP interface comes alive on network; begin LCP negotiations:

Send Configure-Request →
← Send Configure-Request
← Send Configure-ACK
Send Configure-ACK →

2. LCP opened; begin authentication phase, PAP or CHAP:

PAP*		**CHAP***
Send Authenticate-Request →		Challenge →
← Send Authenticate-ACK		← Response
		Response Match →

*Shows Router A initiating authentication. Router B can also initiate authentication.

3. Authentication complete; begin NCP negotiations:

Send Configure-Request →
← Send Configure-Request
← Send Configure-ACK
Send Configure-ACK →

4. NCP open; begin transmitting data:

← **Send Data** →

Figure 1-2. PPP Interface Initialization

Authenticating the PPP Link: PAP and CHAP

In the authentication phase of PPP initialization, one or both peer routers enable either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP).

Password Authentication Protocol

PAP imposes network security by requiring the peer router to send a PAP packet that contains a plain-text user identifier and password to the originating router before the interface can advance to the network layer protocol phase.

If PAP fails, the network administrator must change the identifier and password on both peer routers and disable and re-enable LCP to reinitialize the line.

Challenge Handshake Authentication Protocol

CHAP imposes network security by requiring that the peers share a plain-text secret. The originating peer sends a challenge message to its receiving peer. The receiving peer responds with a value it calculates on the basis of knowing the secret. The first peer then matches the response against its own calculation of what the response should be. If the values match, it sends a success message, and the LCP establishes the link.

CHAP uses an incrementally changing identifier and a variable challenge value to provide network security. It also allows for repeated challenges at intervals that either router on a link can specify. A router may transmit challenge packets not only during the link establishment phase, but also at any time during the network layer protocol phase to ensure that the connection retains its integrity.

If CHAP fails, the network administrator must change the identifiers and secret on both peer routers and disable and re-enable LCP to reinitialize the line.

Note: *For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bring up bandwidth-on-demand, dial-on-demand, and dial backup lines. In addition, for all dial services, failure of either authentication protocol causes the connection to be dropped, and no intervention from the network administrator is needed.*

Establishing Network Connections

PPP uses various network control protocols to determine the values of parameters during the final phase of PPP initialization, network layer negotiations. Like the LCP, each network control protocol allows peer routers to negotiate various network options over the data link by transmitting Configure-Request, Configure-ACK, Configure-NAK, and Configure-Reject packets.

Network options include which network addresses to use and which media types to bridge. Once both peer routers agree upon network options, the network control protocol reaches the opened state. The routers then begin transmitting user data packets for any upper-layer protocols over the link.

Datagram Encapsulation

Before transmitting data across the link, PPP encapsulates data in a frame similar to a High-level Data Link Control (HDLC) frame (Figure 1-3).

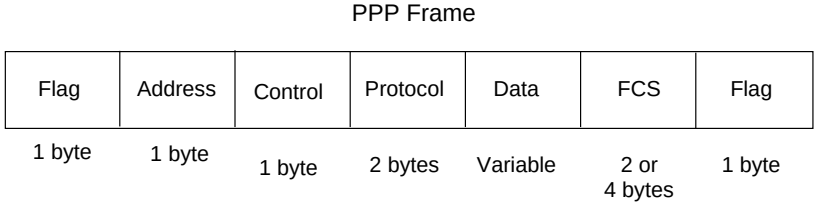


Figure 1-3. PPP-Encapsulated Frame

The parts of the PPP frame function as follows:

- The Flag field marks the beginning and end of a frame. Peers on synchronous lines exchange flags continuously when there are no frames to transmit.
- The Address field indicates which device originated the frame.
- The Control field shows the frame type (information or administrative).
- The Protocol field indicates the operative network layer protocol.
- The Data field contains the data one link sends to the other. Its length is less than or equal to the MTU line size. The default maximum length is 1594 bytes; LCP negotiations determine the actual length.
- The Frame Check Sequence (FCS) shows the sequence order of the frame; router hardware computes the FCS. A 16- or 32-bit Cyclic Redundancy Check (CRC) is at the end of each frame.

Monitoring the PPP Link

To ensure that the router can successfully transfer data, PPP monitors the quality of the point-to-point link with Link Quality Monitoring (LQM) and Link Quality Report (LQR) packets. PPP supports LQM over standard synchronous interfaces only. PPP does not support LQM over high-speed serial interfaces (HSSI). BNX software, however, *does* support LQM and LQR over HSSI interfaces.

Note: *PPP uses LQM and LQR only if you set the Link Quality Protocol parameter to LINKQR. The default is None.*

When you enable link quality monitoring through the Link Quality Protocol, you are turning on monitoring only for the local router. For link quality monitoring to be operational, it only has to be enabled on one side of the link. If two routers are configured for different link quality reporting periods, they negotiate to the lower value, so that the LQR period will be the same on both sides of the link.

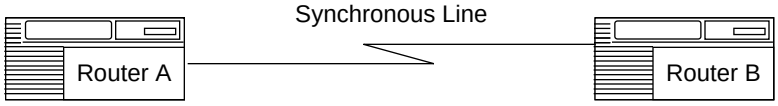
LQR packets contain counters of incoming and outgoing data packets for the routers on each side of the link. Each time a router receives an LQR packet, PPP uses that packet to calculate the outbound link quality (the percentage of packets the router transmitted that its peer successfully receives) and the inbound link quality (the percentage of packets that the peer transmitted that this router successfully receives).

After five LQR reporting periods, PPP averages the inbound and outbound link quality and compares these values against a user-specified threshold. This is a rolling average. After the first five LQR reporting periods, PPP acquires the data from the next period and drops the oldest data. Then it computes the link quality average for that set of five LQR periods, and so on.

If either the inbound or outbound link quality average drops below the threshold, PPP brings down the link. The driver software automatically brings the link back up and renegotiates the connection. PPP monitors the link control packets flowing over the connection and resumes network control protocol packet traffic when the link quality improves.

For example, in Figure 1-4, the acceptable outbound and inbound link quality configured on Router A for the PPP interface is 100 percent. After five LQR periods, Router A calculates the outbound and inbound link quality averages and determines that the inbound link quality average is below the 100 percent threshold (in this case, 90 percent). As a result, Router A disables the link.

Note: *Echo-Requests are disabled by default and are in no way related to link quality reporting.*



LQR Period	Packets Router A Transmitted	Packets Router B Received	Outbound Link Quality Router A
1	100	100	100%
2	100	100	100%
3	100	100	100%
4	100	100	100%
5	100	100	100%

Outbound average after 5 LQR periods = 100%

LQR Period	Packets Router A Received	Packets Router B Transmitted	Inbound Link Quality Router A
1	90	100	90%
2	90	100	90%
3	90	100	90%
4	90	100	90%
5	90	100	90%

Inbound average after 5 LQR periods = 90%

Figure 1-4. Link Quality Monitoring from Router A's Perspective

In addition to LQR packets, PPP periodically transmits Echo-Request packets (when Echo-Request is enabled). If the peer transmits a user-specified number of Echo requests before receiving an Echo reply from its peer router, the router disables the link and restarts.

Chapter 2
Implementation Notes

This chapter addresses special configuration features of Bay Networks Point-to-Point Protocol (PPP) services. It also contains basic guidelines on configuring PPP interfaces.

PPP Data Compression

The Bay Networks data compression feature lets you reduce line costs and improve response times over wide area networks (WANs) running PPP.

Our data compression eliminates redundancies in data streams. When you use compression on your network, bandwidth efficiency improves, and you can transmit more data over a given amount of network bandwidth.

Bay Networks data compression services for PPP include

- Software-based compression for all platforms and all serial interfaces
- Hardware-based data compression for PPP networks that use the octal synchronous link module for the Backbone Node (BN®), using only FRE®2 processors. Bay Networks provides hardware compression as an optional daughterboard that attaches to the octal synchronous link module.

You can use data compression on all PPP circuits, including multiline, multilink, bandwidth-on-demand, dial-on-demand, and dial backup lines. When you use compression on a bandwidth-on-demand, dial-on-demand, or dial backup circuit, the data compression feature automatically configures or deletes compression as lines are added to or removed from the circuit.

For complete descriptions of hardware and software data compression, descriptions of compression parameters, and instructions for configuring compression over a PPP interface, see *Configuring Data Compression Services*.

PPP Dial Services Support

Bay Networks dial services offer access to switched networks through dial-up line connections (also called *switched lines*) that are active only when you choose to use them. In contrast, a leased line is always available. If you transmit limited amounts of data, or if your data transmission is intermittent, dial services may let you run your network effectively and economically.

Site Manager automatically configures PPP on the lines that you select for dial services. PPP, with either CHAP or PAP, implements a router identification mechanism that dial services require.

Bay Networks provides three types of dial services: bandwidth-on-demand, dial-on-demand, and dial backup. For information on how to configure bandwidth-on-demand, dial-on-demand, and dial backup lines, see *Configuring Dial Services*.

Bandwidth-on-Demand

Bandwidth-on-demand uses secondary, dial-up lines to augment a primary, leased line (or lines) or an initial dial-on-demand line when the primary line experiences congestion. Congestion occurs when traffic volume exceeds the configured congestion threshold. Bandwidth-on-demand brings up these secondary lines one at a time, as needed, up to a maximum of four lines (including the primary lines). When congestion abates, the secondary lines become inactive.

Dial-on-Demand

Dial-on-demand enables you to establish a circuit “on demand” as opposed to having a leased-line connection, which is always available. By using a circuit on a demand basis, you can have a network connection only when you need it and significantly reduce your line costs.

Dial Backup

If a primary PPP, Frame Relay, or standard line fails and you have enabled dial backup, the router automatically establishes a backup line and data transmission continues.

PPP Multiline

Bay Networks PPP services include support for the multiline feature, which lets you configure a single circuit that consists of one or more WAN data paths. A data path is a logical point-to-point channel that is a permanent (leased) line. Multiline provides both increased fault tolerance and greater bandwidth between two sites.

Refer to the section "Differences between Multi*line* and Multi*link*" on page 2-7 for a comparison of these features. For more information about the Bay Networks multiline feature, see *Configuring Line Services*. For information on configuring PPP Multiline over HSSI interfaces within the BNX environment, refer to *Configuring Customer Access (BNX Software)*.

PPP Multilink

Note: *BNX software does not support the PPP multilink feature. If you use BNX, ignore this and the following four sections.*

The multilink feature of PPP provides capabilities beyond those of multiline circuits. The major characteristics of multilink include the ability to

- Use lines that have different speeds, proportionally distributing traffic over those lines
- Balance traffic load and maintain packet sequence
- Use switched lines (such as ISDN-B channels) as well as leased lines
- Monitor traffic volume

Configurations with bandwidth-on-demand, which can activate additional lines in response to increased traffic, can find these features particularly useful.

Multilink is available on the following platforms:

- BLN®/BCN®
- LN®/CN®
- AFN®
- AN™
- ASN™

Using PPP Multilink

The routers at each end of a PPP link (that is, a logical communications line) are called *peers*. A link is an individual communication channel between two peers. Typical links include one ISDN B channel, an aggregation of T1 DS0s, one dial-up modem connection, and one leased T1 line.

Links can be either leased or switched lines. All links must have the same datalink encapsulation (PPP), and all links must have the same maximum transmission unit (MTU). On non-ISDN lines, you must configure the clock speed.

When you enable multilink, you can configure a set of links between two peers into a single "bundle," which can consist of up to four links, possibly of different bandwidths. With multilink configured, leased lines in a bundle can be on different router slots. Multilink distributes traffic over each logical line in a bundle in an amount roughly proportional to the effective bandwidth of the link.

With multilink and bandwidth-on-demand enabled, you can configure one side of the link as the congestion monitor. This router monitors network traffic and line usage. When the traffic exceeds a user-specified threshold, the bandwidth-on-demand monitor can initiate the bringing up of a secondary line.

Figure 2-1 shows a configuration that uses the multilink feature.

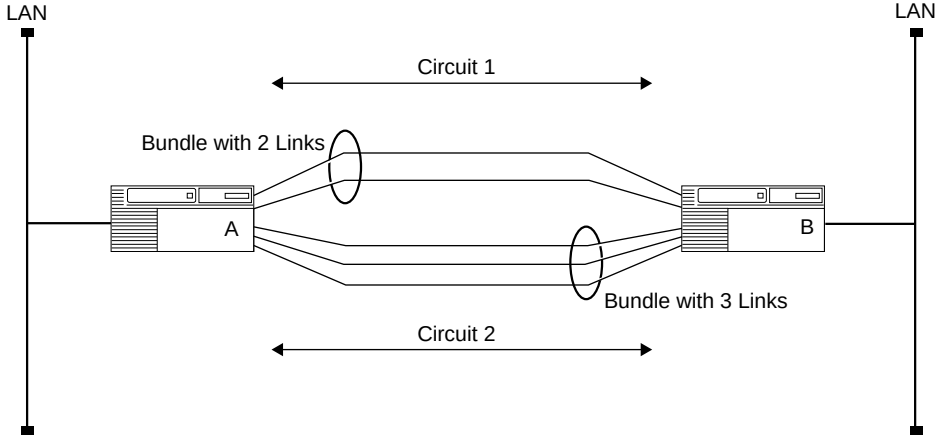


Figure 2-1. Multilink Circuits

As Figure 2-1 shows, you can have more than one multilink bundle active between two peer routers. Each bundle is a separate circuit; that is, a separate logical connection.You cannot share links between circuits. Once you have configured a circuit for multilink or bandwidth-on-demand operation, it always uses PPP multilink encapsulation.

All lines in a circuit must negotiate and perform multilink. You cannot pair non-multilink lines with multilink lines in a circuit. Multilink can resequence packets sent over different lines of the link, but Version 10.0 does not support packet fragmentation and reassembly.

You can use the multilink feature over the following physical media:

- V.35
- MCT1/MCE1
- ISDN B-channel drivers
- Raise-DTR modems
- V.25bis modems

Compatibility with Previous Versions

A multi*link* circuit using PPP cannot communicate with a router running a version earlier than 9.0 because pre-9.0*x* versions use a multi*line* circuit in which LCP is run on only one line. In this situation, therefore, you must use uniline PPP.

Balancing Traffic Loads

In a configuration with multilink enabled, a sending router divides the outbound traffic among all the lines in the bundle, keeping each packet intact. The configured external clock speed of each line determines the proportion of the total traffic each receives. For example, pairing a 9600 bit/second line with an ISDN B-channel yields a clock-speed ratio of roughly 1:6.8. That is, for every packet sent over the slower link, the router can send about seven packets over the faster link.

On the receiving end, multilink resequences packets arriving on different links using the sequence number from the multilink header. Gaps in the ordering may occur, however, when packets are corrupted or otherwise lost or when they arrive after packets with later sequence numbers. To minimize this situation, multilink buffers out-of-sequence packets in case the preceding sequence numbered packets arrive shortly after the later-numbered packets.

Configuring Multilink Operation

You configure a PPP multilink circuit by selecting the appropriate value in the PPP circuit entry record for the intended circuit. This parameter controls whether the local side of the bundle attempts to negotiate the multilink protocol, and whether the local circuit operates as the congestion monitor for bandwidth-on-demand. The congestion monitor locally monitors traffic congestion on the circuit. Only one side of any connection should be the congestion monitor.

Protocol Prioritization

Note: *BNX software uses a different protocol prioritization mechanism from that described in this section. For information on BNX traffic prioritization and congestion control mechanisms, refer to* Configuring Customer Access (BNX Software).

When you configure a router, you can prioritize the different types of traffic sent across a synchronous line. This process is called *protocol prioritization*. The ability to prioritize traffic is important because some types of operations require faster responses than other types. For example, PPP control messages must have precedence over other types of data.

When you select PPP on a circuit, Site Manager automatically enables protocol prioritization without specifying any filters.

With the multi*line* feature, you can configure both priorities and filters. For more information about protocol prioritization see *Configuring Traffic Filters and Protocol Prioritization*.

The multi*link* feature uses the automatically enabled functions of protocol prioritization, but only for interrupt queuing. You cannot specify either traffic filters or priorities. Multilink assigns the highest (that is, interrupt-level) priority to link control packets, treating all other traffic as normal priority. This gives PPP control messages precedence over other types of data while preserving the packet sequencing.

Differences between Multi*line* and Multi*link*

Both multiline and multilink use circuits consisting of one or more data paths between two peer routers. Each has its special characteristics and advantages, described in the following paragraphs and summarized in Table 2-1.

Table 2-1. Comparing Multiline and PPP Multilink

Feature	Multiline	PPP Multilink
Advantages	• Fault tolerance • Bandwidth availability	• Fault tolerance • Bandwidth availability • Uses all lines in the bundle for greatest speed and efficiency
Number of physical lines/ circuit	• Up to 31 concurrent data paths/group • Data paths can either be physical or logical lines (multiple independent data paths running over a single physical interface).	Up to 4 lines/bundle
Grouped/bundled data paths	The data paths that together make up a multiline circuit must share the same speed, MTU, and encapsulation method.	Lines in a bundle can have different speeds.
Line types	Can use leased lines.	Can use leased as well as switched lines.
Protocol prioritization	Automatically enabled. User can specify protocol priority and/or traffic filters.	Automatically enabled. Not user configurable. Automatically assigns highest (interrupt) priority to LCP packets and assigns all others normal priority.
Used with these data link types	• Bay Networks standard synchronous • Frame Relay direct mode • PPP	PPP (only)

Table 2-1. Comparing Multiline and PPP Multilink *(continued)*

Feature	Multiline	PPP Multilink
Media supported	• Synchronous • T1/E1 • MCE1/MCT1 • HSSI	• Synchronous • T1/E1 • MCE1/MCT1 • HSSI • ISDN B-channel drivers • Raise-DTR/V.25bis modems
Packet resequencing	Depends on the path selection: • With address-based selection (the default), packets always arrive in sequence. • With random path selection, packets traveling on different paths can arrive at their destination out of sequence.	Multilink maintains the sequence of packets sent over different lines of the link.
Support for bandwidth-on-demand	No	Yes
Miscellaneous	• Address-based selection does not always result in even traffic distribution across all data paths. • Random selection provides for even traffic distribution.	• All lines in a circuit must negotiate and perform multilink. • You cannot use non-multilink lines in a circuit with multilink lines. • All data packets sent over a PPP multilink circuit travel as multilink packets.

PPP Synchronous Line Parameters

If you enable PPP on a circuit, PPP automatically sets the following synchronous line parameters (Table 2-2).

Table 2-2. PPP Synchronous Line Parameter Values

Parameter	Value
BOFL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	PPP

For more information on these parameters, refer to *Configuring Routers* or *Configuring Customer Access (BNX Software),* as appropriate for your platform.

PPP Software Incompatibilities

If you need to configure PPP to run over a point-to-point connection between a Version 5.*x* and a Version 10.0 router, read this section.

Note: *This section is not relevant for BNX software.*

Version 5.*x* router software uses a Bay Networks proprietary implementation of PPP. Version 7.*x*, Version 8.*x*, Version 9.*x*, and Version 10.0 routers support a new implementation of PPP. The new implementation complies with the established requirements of the following Internet RFCs: 1332, 1333, 1334, 1378, 1552, 1638, 1661, 1662, 1762, 1763, and 1764. Version 10.0 routers also support the multilink feature, described in RFC 1717.

With the different implementations of PPP, each adhering to a different set of RFCs, the following functions will not work between a Version 5.*x* and a Version 9.*x* or Version 10.0 router:

- Link Quality Monitoring (LQM)
- Source-routing over Token Ring networks

For communication over a synchronous line between a Version 5.*x* and a Version 9.*x* or Version 10.0 router, each running PPP, make the following configuration checks:

- On the Version 9.*x* or Version 10.0 router
  - The type of synchronous line service (MIB object ID 1.3.6.1.4.1.18.3.4.5.1.18, *wfSyncService*) must have a value of *Transparent*. (This is the default setting for the Service parameter in the Edit Sync Parameters window. To access the parameter through the Configuration Manager, click on the appropriate sync connector and select Edit Line Details.)
- On the Version 5.*x* router
  - The LQM Time parameter must have a value of 0, which disables Link Quality Monitoring on the Version 5.*x* router.

— The Quality of Service parameter must have a value of LLC1, the default setting.

For information on how to check these Version 5.*x* parameters, refer to your Version 5.*x* configuration guide.

For further information on configuring different versions of routers to assure software compatibility, see *Upgrading Routers from Version 5 to Version 10.0* and *Upgrading Routers from Version 7-8.xx to Version 10.0*.

Configuring IP to Run over PPP Interfaces

When you enable numbered Internet Protocol (IP) support on a PPP interface, you must also configure an adjacent host entry for the peer router. See *Configuring IP Services* for instructions on configuring an adjacent host entry.

Disabling Network Control Protocols

To stop traffic from routing over a PPP interface, either

- Disable the Network Control Protocol (NCP) for the upper-level routing protocol.

  For example, if you disable the NCP for IP, even though IP is still enabled on the interface, it is no longer able to route traffic over the interface.

  To disable the NCP for IP, you set the IP Enable parameter to Disable. See "Editing PPP Interface Parameters" in Chapter 4 for instructions on disabling NCP parameters.

- Disable the upper-level routing protocol itself.

  If you disable the routing protocol running on top of the PPP interface, Site Manager disables the NCP for the routing protocol automatically. For example, if you disable IP on an interface, Site Manager disables the NCP for IP as well.

Calculating and Viewing Line Statistics

You can optionally calculate receive percentage statistics on the active multilink circuits connecting two peers. To do this, you must use the Technician Interface to enable the *wfPppMlStatsCalcPercent* parameter in the *wfPppMlStatsEntry* MIB. When you enable this feature, the router calculates the percentage of data successfully received per line. By default, this parameter is set to disabled.

The Active Circuit parameter, *wfPppLineActiveCct* in the *wfPppLineEntry* MIB, shows the actual PPP circuit associated with each line. The purpose of this parameter is to easily extract the line numbers within a given multilink circuit and vice-versa.

For all line types, the default value of *wfPppLineActiveCct* is 0xffff (equivalent to a value of -1). The actual value depends on whether the line is leased or switched.

- For a leased line, the parameter *wfPppLineActiveCct* always shows the correct active circuit number.
- For an active (up) switched line, this parameter contains the actual circuit associated with the line. This applies to dial-on-demand, dial backup, bandwidth-on-demand, and demand groups. When a switched line is brought down, this parameter reverts to the default value.

After you enable *wfPppMlStatsCalcPercent*, the router requires some transient time before the percentage readings are accurate; that is, it must collect sufficient data and do the calculations based on that data. The time required for accurate calculations depends on a variety of factors, including the line speed and the amount of data received.

To view the statistics, use the Technician Interface to turn on logging for the PPP entity before enabling the percentage calculation. Set the *wfPppMlStatsDebug* parameter in the *wfPppMlStatsEntry* MIB to a value of 1. The router then dumps the received percentages for all lines of that multilink circuit to the log file. You can view the log file using the standard log viewing commands in the Technician Interface. For information on how to do this, refer to *Using Technician Interface Software*.

You can use these statistics to determine how well each line in a multilink bundle is performing and to pinpoint potential trouble spots. For best performance on a generally stable circuit, you should disable the statistics calculation unless you have a particular reason for enabling it.

Chapter 3
Enabling PPP Service

This chapter describes how to enable PPP service. It assumes you have read *Configuring Routers* or *Configuring Customer Access (BNX Software)*, as appropriate for your platform, and have

1. Opened a configuration file
2. Specified router hardware, if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling PPP

When you enable PPP service, you do not have to configure any PPP parameters. The Configuration Manager supplies default values for all PPP parameters. If you want to edit the default values, refer to Chapter 4, "Editing PPP Parameters."

Enabling PPP on an Interface

To enable PPP on an interface, complete the following steps.

1. **Select PPP from the WAN Protocols menu; this menu appears after you select a link or net module connector that requires a WAN circuit.**

   If you are running router (as opposed to BNX) software, Protocol prioritization is enabled automatically when you select PPP. For detailed information on protocol prioritization, refer to *Configuring Traffic Filters and Protocol Prioritization.*

2. **Click on OK to enable default PPP service.**

   The Configuration Manager displays the Select Protocols window. Refer to the appropriate protocol-specific guides for information on enabling the protocols you want to run on this interface.

Chapter 4
Editing PPP Parameters

This chapter provides information on how you can edit, or customize, the parameters for the PPP interfaces that you configure on the router.

For each PPP parameter that you configure, this chapter gives the default setting, all valid parameter options, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID.

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: *The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.*

After you enable PPP, you can edit all PPP parameters from the Configuration Manager window (Figure 4-1). For instructions on using Site Manager to access this window, refer to *Configuring Routers* or *Configuring Customer Access (BNX Software)*, as appropriate for your platform.

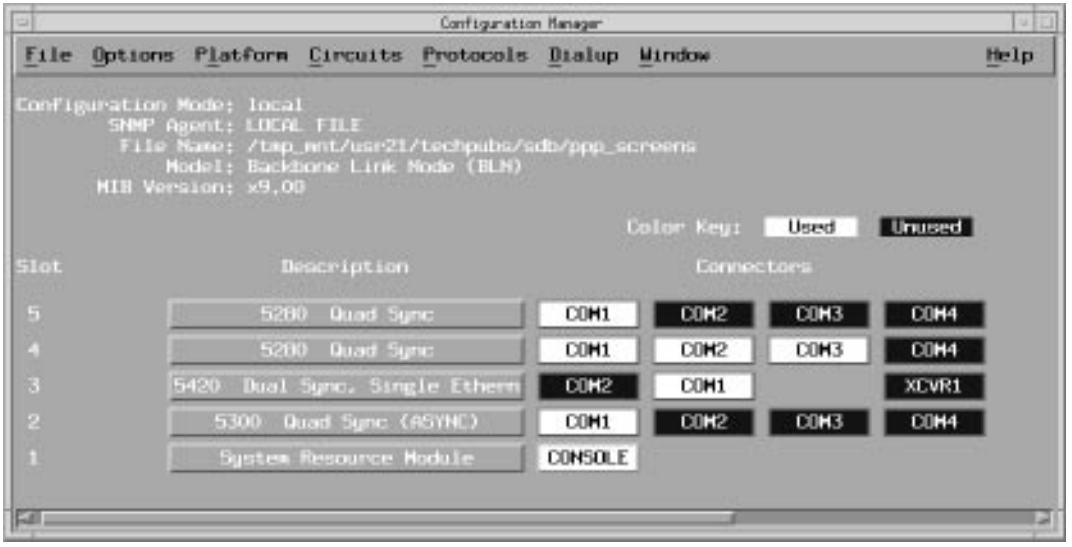

Configuration Manager
File Options Platform Circuits Protocols Dialup Window Help
Configuration Mode: local
SNMP Agent: LOCAL FILE
File Name: /tmp_mnt/usr21/techpubs/sdb/ppp_screens
Model: Backbone Link Node (BLN)
MIB Version: x9.00
Color Key: Used Unused
Slot
Description
Connectors
5 5200 Quad Sync COM1 COM2 COM3 COM4
4 5200 Quad Sync COM1 COM2 COM3 COM4
3 5420 Dual Sync, Single Ethern COM2 COM1 XCVR1
2 5300 Quad Sync (ASYNC) COM1 COM2 COM3 COM4
1 System Resource Module CONSOLE

Figure 4-1. Configuration Manager Window

Editing PPP Interface Parameters

To edit the PPP interface-specific parameters, begin at the Configuration Manager window shown in Figure 4-1 and proceed as follows:

1. **Select Protocols→PPP→Interfaces.**

   The PPP Interface Lists window appears (Figure 4-2). You must scroll the list to see all the parameters on this window.

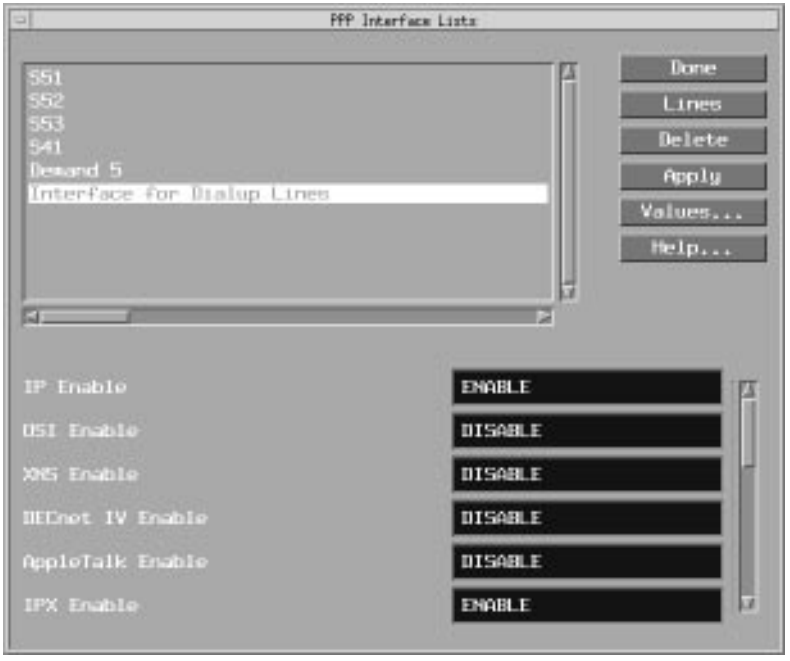


Figure 4-2. PPP Interface Lists Window

2. **Select the PPP interface that you want to edit.**
3. **Edit those parameters you want to change, referring to the descriptions following this procedure for guidelines.**

   If you change any of the following parameters, you must force Link Control Protocol (LCP) renegotiation on the interface for your changes to take effect.

   - Remote IP Address
   - IPX Remote Node Number
   - Remote AppleTalk Node
   - AppleTalk Routing Protocol
   - Bridge Ethernet
   - Bridge FDDI
   - Bridge Token Ring

You must disable and then re-enable the corresponding network control protocol to implement your changes. Therefore, after making all your changes to any of the parameters listed in the previous steps, but *before* proceeding to Step 4, do the following:

a. **Set the corresponding network control protocol parameter(s) to Disable.**

   For example, if you change the Remote IP Address parameter, set the IP Enable parameter to Disable; if you change the Remote AppleTalk Node parameter, set the AppleTalk Enable parameter to Disable.

b. **Click on Apply.**

c. **Reset the corresponding network control protocol parameters to Enable.**

4. **Click on Apply to implement your changes.**

5. **Click on Done to exit the window.**

If you configure bandwidth-on-demand, dial-on-demand, or dial backup services, you see a special PPP record for demand or backup circuits in the PPP Interface Lists window that reads:

```
Interface for Dialup Lines
```

This is a generic PPP record that dial services circuits use for identification purposes.

PPP Interface Parameter Descriptions

Use the following guidelines to configure the parameters in the PPP Interface Lists window.

Note: *In BNX software environments, only the IP Enable parameter is meaningful. In the BNX environment, ignore all other PPP interface parameters.*

Parameter:	**IP Enable**
Default:	If you enable IP support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for IP. This parameter does *not* enable or disable IP routing services for the interface; it affects the network control protocol for IP. However, disabling the network control protocol for IP stops IP traffic from being routed over this interface.
Instructions:	To stop IP traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.12

Parameter:	**OSI Enable**
Default:	If you enable Open Systems Interconnect (OSI) support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for OSI. This parameter does *not* enable or disable OSI routing services for the interface; it affects the network control protocol for OSI. However, disabling the network control protocol for OSI stops OSI traffic from being routed over this interface.
Instructions:	To stop OSI traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.13

Parameter:	**XNS Enable**
Default:	If you enable XNS support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for XNS. This parameter does *not* enable or disable XNS routing services for the interface; it affects the network control protocol for XNS. However, disabling the network control protocol for XNS stops XNS traffic from being routed over this interface.
Instructions:	To stop XNS traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.14

Parameter:	**DECnet IV Enable**
Default:	If you enable DECnet IV support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for DECnet IV. This parameter does *not* enable or disable DECnet IV routing services for the interface; it affects the network control protocol for DECnet IV. However, disabling the network control protocol for DECnet IV stops DECnet IV traffic from being routed over this interface.
Instructions:	To stop DECnet IV traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.15

Parameter:	**AppleTalk Enable**
Default:	If you enable AppleTalk support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for AppleTalk. This parameter does *not* enable or disable AppleTalk routing services for the interface; it affects the network control protocol for AppleTalk. However, disabling the network control protocol for AppleTalk stops AppleTalk traffic from being routed over this interface.
Instructions:	To stop AppleTalk traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.16

Parameter:	**IPX Enable**
Default:	If you enable Internet Packet Exchange (IPX) support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for IPX. This parameter does *not* enable or disable IPX routing services for the interface; it affects the network control protocol for IPX. However, disabling the network control protocol for IPX stops IPX traffic from being routed over this interface.
Instructions:	To stop IPX traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.17

Parameter:	**Bridge Enable**
Default:	If you enable the bridge on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for the bridge. This parameter does *not* enable or disable bridging services for the interface; it affects the network control protocol for the bridge. However, disabling the network control protocol for the bridge stops traffic from being bridged over this interface.
Instructions:	To stop traffic from being bridged over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.18

Parameter:	**VINES Enable**
Default:	If you enable VINES support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables the network control protocol for VINES. This parameter does *not* enable or disable VINES routing services for the interface; it affects the network control protocol for VINES. However, disabling the network control protocol for VINES stops VINES traffic from being routed over this interface.
Instructions:	To stop VINES traffic from being routed over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.19

Parameter:	**CCP Enable**
Default:	If you enable data compression on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Options:	Enable | Disable
Function:	Enables or disables data compression. This parameter does *not* enable or disable data compression for the interface. However, disabling the Compression Control Protocol (CCP) stops data compression over this interface.
Instructions:	To stop compression over this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.49

Parameter:	**Remote IP Address**
Default:	0.0.0.0
Options:	Any valid IP address
Function:	Specifies the IP address the peer router should use. This interface includes this IP address in NCP negotiations.
Instructions:	If you want to specify an IP address for the peer router, enter it here. If this interface has been up and running, you must also set the IP Enable parameter to Disable, click on Apply, and then reset the IP Enable parameter to Enable to implement your changes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.22

Parameter:	**IPX Network Number**
Default:	None
Options:	Any valid, unique, unreserved network number. This number must be a string of up to eight hexadecimal characters. (0xffffffff is invalid.)
Function:	Specifies a network number used to negotiate the link. The negotiated number must be unique. It cannot be a previously assigned network number. Note that both sides of the link do not have to have the same network number; PPP negotiates the higher of the two numbers. Note also that the negotiated number may be 0 (that is, the IPX network number is 0 on both sides of the link). In this case, IPX defines the link's network number.
Instructions:	Enter a valid IPX network number for each PPP interface. Be aware that the value for this parameter depends on the IPX configuration for this interface. For information about IPX and PPP interaction, see *Configuring IPX Services*.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.24

Parameter:	**IPX Remote Node Number**
Default:	None
Options:	Any valid IPX node number
Function:	Specifies the IPX node number the peer router should use. This interface includes this IPX remote node number in NCP negotiations.
Instructions:	If you want to specify an IPX node number for the peer router, enter it here. If this interface has been up and running, you must also set the IPX Enable parameter to Disable, click on Apply, and then reset the IPX Enable parameter to Enable to implement your changes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.26

Parameter:	**Remote AppleTalk Node**
Default:	None
Options:	Any valid AppleTalk node number
Function:	Specifies the AppleTalk node number the peer router should use. This interface includes this AppleTalk node number in NCP negotiations.
Instructions:	If you want to specify an AppleTalk node number for the peer router, enter it here. If this interface has been up and running, you must also set the AppleTalk Enable parameter to Disable, click on Apply, and then reset the AppleTalk Enable parameter to Enable to implement your changes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.36

Parameter:	**AppleTalk Routing Protocol**
Default:	RTMP
Options:	RTMP (Routing Table Maintenance Protocol)
Function:	Specifies the AppleTalk routing update protocol that this interface wants the peer router to use. This interface specifies AppleTalk RTMP as the routing update protocol in NCP negotiations.
Instructions:	Accept the default, RTMP.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.38

Parameter:	**Bridge Ethernet**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this PPP interface accepts bridged traffic that is Ethernet encapsulated, then forwards it over the PPP network.
Instructions:	Set to Disable if you do not want the PPP interface to accept bridged, Ethernet-encapsulated frames. If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, click on Apply, and then reset the Bridge Enable parameter to Enable to implement your changes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.40

Parameter:	**Bridge FDDI**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this PPP interface accepts bridged traffic that is FDDI encapsulated, then forwards it over the PPP network.
Instructions:	Set to Disable to refuse bridged, FDDI-encapsulated frames on this PPP interface. If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, click on Apply, and then reset the Bridge Enable parameter to Enable to implement your changes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.42

Parameter:	**Bridge Token Ring**
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this PPP interface accepts bridged traffic that is Token Ring encapsulated, then forwards it over the PPP network. The Token Ring network must support source routing; the router expects all Token Ring-bridged frames to be source routed.
Instructions:	Set to Disable if you do not want the PPP interface to accept bridged, Token Ring-encapsulated frames. If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, click on Apply, and then reset the Bridge Enable parameter to Enable to implement your changes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.44

Parameter:	**PPP Mode**
Default:	Multilink for a demand or bandwidth-on-demand circuit
	Normal for a nonmultilink circuit
Options:	Multilink | Monitor for a demand or bandwidth-on-demand circuit
	Normal | Multilink for all other circuit types
Function:	Specifies the type of multiline or multilink connection on this interface.
Instructions:	The set of available options depends on the type of circuit you've configured.
	Accept the default or choose one of the following values, depending on what options are available for the circuit you're configuring:
	Select Normal for a nonmultilink circuit.
	Select Multilink to enable the multilink feature.
	Select Monitor to designate the local router as the multilink monitor.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.50

Parameter:	**Max Links**
Default:	4 (links)
Range:	1 to 4
Function:	This parameter is active only for multilink. It specifies the maximum number of links (both leased and switched lines) allowed in the multilink bundle for this circuit at any one time.
Instructions:	Accept the default, 4, or enter a value in the range 1 to 4. If this is not a multilink circuit, leave this parameter blank.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.58

Parameter:	**Max Buffers**
Default:	30 (buffers)
Range:	10 to 60 (buffers)
Function:	This parameter is active only for multilink. It specifies the maximum allowable number of buffers stored by multilink for this circuit. The choice depends on the amount of memory available for buffers, the likelihood of delays in the arrival of packets, and the amount of total network traffic, among other variables. In general, a higher number uses more memory but allows more latitude for late-arriving packets.
Instructions:	Accept the default, 30, or specify a value in the range 10 to 60. If you experience buffer resource problems, try setting this parameter to a lower value. You can determine whether buffer resource problems exist by using the Site Manager Statistics feature or by using the Technician Interface to check the number of times the number of buffers needing to be stored exceeded the number of buffers available (the MIB object *wfPppMlStatsExceededBufferMax*, accessible through the Technician Interface, counts these occurrences).
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.64

Editing PPP Line Parameters

To edit the PPP line-specific parameters, begin at the Configuration Manager window shown in Figure 4-3 and proceed as follows:

1. **Select Protocols→PPP→Interfaces.**

   The PPP Interface Lists window appears (refer to Figure 4-2).

   If you are configuring a bandwidth-on-demand, dial-on-demand, or dial backup line, and if you want to configure CHAP Local Name or PAP ID for identification purposes, select the Interface for Dialup Lines interface.

2. **Click on Lines.**

   The PPP Line Lists window appears (Figure 4-3).

Figure 4-3. PPP Line Lists Window

3. **Select the PPP line that you want to edit.**
4. **Edit those line parameters that you want to change, referring to the descriptions following this procedure for guidelines**

   If you change any of the following parameters, you must force LCP renegotiation on the interface for your changes to take effect.

   - Echo-Reply Acceptable Loss
   - Max Configure-Requests
   - Max Terminate-Requests
   - Max Configuration Failure Count
   - Local Authentication Protocol
   - Local PAP ID
   - Local PAP Password
   - Remote PAP ID
   - Remote PAP Password
   - Link Quality Protocol
   - Peer Link Quality Report Timer
   - LQR Reporting Period
   - CHAP Secret
   - CHAP Local Name
   - CHAP Periodic Timer

   You must disable and then re-enable, the corresponding network control protocol to implement your changes. Therefore, after making all your changes to any of the parameters listed in the previous steps, but *before* proceeding to Step 5, do the following:

   a. **Set the Enable (LCP) parameter to Disable.**
   b. **Click on Apply.**
   c. **Reset the Enable (LCP) parameter to Enable.**

5. **Click on Apply to implement your changes.**
6. **Click on Done to exit the window.**

PPP Line Parameter Descriptions

Use the following guidelines to configure the parameters in the PPP Line Lists window.

Parameter:	**Enable (LCP)**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables the Link Control Protocol (LCP) on the PPP interface. Disabling this parameter generates a “close” event to LCP. Similarly, enabling this parameter generates an “open” event to LCP.
Instructions:	To disable LCP on this interface, set this parameter to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.2

Parameter:	**Restart Timer in Seconds**
Default:	3 (seconds)
Range:	1 to 1000
Function:	Specifies the number of seconds that the Restart Timer waits before retransmitting data.
Instructions:	Accept the default value of 3.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.7

Parameter:	**Seconds between Xmit of Echo-Request**
Default:	0 (seconds)
Range:	0 to 100
Function:	Specifies the number of seconds that the router waits between the transmission of Echo-Request packets. A value of 0 means that this parameter is turned off.
Instructions:	Accept the default value of 0 or enter an integer value in the range 0 to 100.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.8

Parameter:	**Echo-Reply Acceptable Loss**
Default:	3 (packets)
Range:	1 to 100
Function:	Specifies the maximum number of unacknowledged Echo-Reply packets that the router will transmit before declaring the point-to-point link down.
Instructions:	Accept the default value of 3. If you enter a different value, you must set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable to implement your change.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.9

Parameter:	**Max Configure-Requests**
Default:	10 (packets)
Range:	1 to 100000
Function:	Specifies the maximum number of unacknowledged Configure-Request packets that the router will transmit before assuming that the peer router on the other end of the link is unable to respond. The link is then brought down. Valid acknowledgments include Configure-ACK, Configure-NAK, or Configure-Reject packets.
Instructions:	Accept the default value of 10. If you enter a different value, you must set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable to implement your change.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.10

Parameter:	**Max Terminate-Requests**
Default:	2 (packets)
Range:	1 to 100
Function:	Specifies the maximum number of unacknowledged Terminate-Request packets that the router transmits before assuming that the peer router on the other end of the link is unable to respond. The valid acknowledgment is a Terminate-ACK packet.
Instructions:	Accept the default value of 2. If you do enter another value, to implement your change set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.11

Parameter:	**Max Configuration Failure Count**
Default:	10
Range:	1 to 100
Function:	Specifies the maximum number of Configure-NAK packets the router sends before sending a Configure-Reject packet for those options that it does not agree with.
Instructions:	Accept the default value of 10. If you enter a different value, you must set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable to implement your change.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.12

Parameter: **Local Authentication Protocol**

Default: CHAP for dialed services

None for all others

Options: None | PASSAUTH | CHAP

Note: *For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bring up demand, backup, and bandwidth lines. You must configure CHAP Local Name, CHAP Secret, PAP ID, and PAP Password through the Dial menu. See* Configuring Dial Services *for details.*

Function: Specifies the type of authentication protocol that this interface uses: none, PAP (Password Authentication Protocol), or CHAP (Challenge Handshake Authentication Protocol).

Instructions: If you do not want to enable security features on this interface, accept the default, None.

To enable Password Authentication Protocol, select PASSAUTH. Then do the following:

— Define the Local PAP ID and Local PAP Password parameters for this interface.

— Set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.

To enable Challenge Handshake Authentication Protocol, select CHAP. Then do the following:

— Define the CHAP Secret, CHAP Local Name, and CHAP Periodic Timer parameters for this interface. Find these parameters by scrolling further through the list of line parameters.

— Set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.15

Parameter:	**Local PAP ID**
Default:	None
Options:	Any text string; maximum 25 characters
Function:	Specifies the PAP ID assigned to this interface. During the interface's authentication phase, all Password Authenticate-Request messages the peer router sends to this interface must include the correct PAP ID. Otherwise, the interface sends an Authenticate-NAK message and the link is not created.
Instructions:	If you have not enabled PAP, ignore this field. If you set the Local Authentication Protocol to PASSAUTH, specify a unique local PAP ID for this interface. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.

Note: *For dial services that use PAP, you must configure the local PAP ID through the Dial menu. See* Configuring Dial Services *for details.*

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.17

Parameter:	**Local PAP Password**
Default:	None
Options:	Any text string; maximum 25 characters
Function:	Specifies the PAP password assigned to this interface. During the interface's authentication phase, all Password Authenticate-Request messages sent to this interface by the peer router must include the correct PAP password. Otherwise, the peer router sends an Authenticate-NAK message and the link is not created.
Instructions:	If you have not enabled PAP, ignore this field. If you set the Local Authentication Protocol to PAPAUTH, specify a unique local PAP password for this interface. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.

Note: *For dial services that use PAP, you must configure local PAP Password through the Dial menu. See* Configuring Dial Services *for details.*

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.18

Parameter:	**Remote PAP ID**
Default:	None
Options:	Any text string; maximum 25 characters
Function:	Specifies the PAP ID assigned to the remote peer router. During the interface's authentication phase, this interface must include the correct Remote PAP ID in all Password Authenticate-Request messages it sends to the peer router, or the peer router sends an Authenticate-NAK message and the link is not created.
Instructions:	If the remote peer does not have PAP enabled, ignore this field. If the remote peer has PAP enabled, specify the remote PAP ID that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.

Note: *For dial services that use PAP, you must configure remote PAP ID through the Dial menu. See* Configuring Dial Services *for details.*

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.19

Parameter:	**Remote PAP Password**
Default:	None
Options:	Any text string; maximum 25 characters
Function:	Specifies the PAP password assigned to the remote peer router. During the interface's authentication phase, this interface must include the correct Remote PAP Password in all Password Authenticate-Request messages it sends to the peer router. Otherwise, the peer router sends an Authenticate-NAK message and the link is not created.
Instructions:	If the remote peer does not have PAP enabled, ignore this field. If the remote peer has PAP enabled, specify the remote PAP password that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.

Note: *For all dial services, you must configure Local PAP ID through the Dial menu. See* Configuring Dial Services *for details.*

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.20

Parameter:	**Enable PAP Fallback**
Default:	Disable
Options:	Enable | Disable
Function:	Enabling this parameter causes a fallback to PAP if you have selected CHAP as the authentication protocol, and an attempt to negotiate CHAP fails.
Instructions:	Select Enable or Disable. Set this parameter to Enable if you are using any of the switched services. Remember that you must use an authentication protocol if you are using bandwidth-on-demand, dial-on-demand, or dial backup.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.32

Parameter:	**Link Quality Protocol**
Default:	None
Options:	None | LINKQR
Function:	Enables or disables the Link Quality Protocol for this interface.
Instructions:	To enable link quality reporting, set this parameter to Link Quality Report. When you enable link quality reporting on one side of the connection, the router on which you enable it is responsible for monitoring link quality for the connection. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.21

Parameter:	**Peer Link Quality Report Timer**
Default:	Enable
Options:	Enable | Disable
Function:	This parameter deals with the *remote* peer, not the local one. The setting determines whether the remote peer runs the Link Quality Report Timer (LQR) for the connection. Setting this parameter enables or disables the remote peer's LQR Timer. The peer whose timer is enabled generates one LQR packet for each interval specified in the LQR Reporting Period parameter. The peer whose timer is disabled verifies that the other peer did, in fact, send an LQR. If three successive LQRs are not received, it disables the connection.
Instructions:	Use this parameter only when you have enabled the Link Quality Protocol parameter. Accept the default, Enable, if you want the peer router to maintain an LQR timer for the interface. Reset this parameter to Disable if you do not want the peer to maintain the LQR timer for the interface. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.22

Parameter:	**LQR Reporting Period**
Default:	3 (seconds)
Range:	1 to 120
Function:	Specifies the maximum number of seconds between the transmission of LQR packets.
Instructions:	Use this parameter only when you enable the Link Quality Protocol parameter. Enter a number representing the interval between the transmission of LQR packets. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.23

Parameter:	**Inbound Link Quality**
Default:	90 (percent)
Range:	0 to 100
Function:	Specifies the minimum acceptable success rate (percentage) of packets the peer router transmits and this router receives on this interface over the last 5 LQR reporting periods. Use this parameter only when you enable the Link Quality Protocol parameter. If the percentage drops below the inbound link quality you specify, the router brings down the link until the percentage increases to an acceptable level. See “Monitoring the PPP Link” in Chapter 1 for more information.
Instructions:	Use this parameter only when you enable the Link Quality Protocol parameter. Accept the default value, 90.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.25

Parameter: **Outbound Link Quality**

Default: 90 (percent)

Range: 0 to 100

Function: Specifies the minimum acceptable success rate (percentage) of packets the router transmits and the peer router receives on this interface. Use this parameter only when you enable the Link Quality Protocol parameter.

If the percentage drops below the outbound link quality you specify, the router brings down the link until the percentage increases to an acceptable level.

See "Monitoring the PPP Link" in Chapter 1 for more information.

Instructions: Use this parameter only when you enable the Link Quality Protocol parameter.

Accept the default, 90.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.27

Parameter: **CHAP Secret**

Default: None

Options: Any text string; maximum 20 characters

Function: Specifies the CHAP secret you assign to this interface. The CHAP secret must be the same on both sides of the link. Both routers on a link must have the same secret to correctly calculate responses to challenges either one of them may send to the other during the authentication process and the network layer negotiation phase.

Note: *For all dial services, you must configure CHAP Secret through the Dial menu. See* Configuring Dial Services *for details.*

Instructions: If you have not enabled CHAP, ignore this field.

If you have enabled CHAP, specify the secret. To implement your changes, set the Enable (LCP) parameter to Disable, click on Apply, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.31

Parameter: **CHAP Local Name**

Default: None

Options: Any text string; maximum 20 characters

Function: A local CHAP Name informs the peers of each other's identity.

Instructions: If you configure CHAP as an authentication protocol, you *must* use CHAP Local Name for router identification on a bandwidth-on-demand, dial-on-demand, or dial backup line. If you do not configure CHAP, you *cannot* use CHAP Local Name for identification; instead, you must configure PAP.

Note: *For all dial services, you must configure CHAP Local Name through the Dial menu. See* Configuring Dial Services *for details.*

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.33

Parameter: **CHAP Periodic Timer**

Default: None

Options: Any number of seconds. Setting this value to 0 disables the timer. A reasonable value for this parameter is 60.

Function: Allows for repeated authentication challenges at an interval (in seconds) that either peer on the link can specify. The timer begins counting when an authentication phase has completed. A new challenge does not begin until the amount of time you specify elapses.

Instructions: Set to 60.

If you have not configured CHAP, ignore this field.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.35

Parameter:	**Allow PAP Reject**
Default:	Disable
Options:	Enable | Disable
Function:	Some peers do not use PAP. If you set this parameter to Enable, your router accepts the Reject message from such a peer and removes PAP from the LCP Configure-Request.
Instructions:	Select Enable or Disable. If you have not configured PAP, ignore this field.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.39

Deleting PPP

To delete PPP from *all* circuits on which it is currently configured, complete the following steps:

1. **From the Configuration Manager window (refer to Figure 4-1), select Protocols➔PPP➔Delete PPP.**

   A window pops up and asks

   ```
   Do you REALLY want to delete PPP?
   ```

2. **Click on OK.**

   Site Manager returns you to the Configuration Manager window. PPP is no longer operating on the router.

Note: *Site Manger does not allow you to delete PPP globally from a router that is running bandwidth-on-demand, dial-on-demand, or dial backup.*

Appendix A
PPP Parameter Default Settings

Tables A-1 and A-2 list the default settings for PPP parameters.

Table A-1. Point-to-Point (PPP) Interface Parameters

Parameter	Default
IP Enable	If you enabled IP support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
OSI Enable	If you enabled OSI support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
XNS Enable	If you enabled XNS support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
DECnet IV Enable	If you enabled DECnet IV support on this interface, then Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
AppleTalk Enable	If you enabled AppleTalk support on this interface, then Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
IPX Enable	If you enabled IPX support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.

(continued)

Table A-1. Point-to-Point (PPP) Interface Parameters *(continued)*

Parameter	Default
Bridge Enable	If you enabled bridging on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
VINES Enable	If you enabled VINES support on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
CCP Enable	If you enabled data compression on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Remote IP Address	0.0.0.0
IPX Network Number	None
IPX Remote Node Number	None
Remote AppleTalk Node	None
AppleTalk Routing Protocol	RTMP
Bridge Ethernet	Enable
Bridge FDDI	Enable
Bridge Token Ring	Enable
PPP Mode	Normal for a nonmultilink circuit Multilink for a multilink circuit
Max Links	4
Max Buffers	30

Table A-2. Point-to-Point (PPP) Line Parameters

Parameter	Default
Enable (LCP)	Enable
Restart Timer in Seconds	3
Seconds between Xmit of Echo-Request	0
Echo-Reply Acceptable Loss	3
Max Configure-Requests	10
Max Terminate-Requests	2
Max Configuration Failure Count	10
Local Authentication Protocol	None
Local PAP ID	None
Local PAP Password	None
Remote PAP ID	None
Remote PAP Password	None
Enable PAP Fallback	Disable
Link Quality Protocol	None
Peer Link Quality Report Timer	Enable
LQR Reporting Period	3
Inbound Link Quality	90
Outbound Link Quality	90
CHAP Secret	None
CHAP Local Name	None
CHAP Periodic Timer	None
Allow PAP Reject	Disable

Appendix B
PPP Statistics

The following table summarizes the PPP statistics you can view from the Site Manager Statistics Manager tool or from the Technician Interface.

Table B-1. PPP Statistics

MIB object name	What it tells you
wfPppMlStatsCircuitID	Circuit number for this instance
wfPppMlStatsHomeSlot	Slot on which this multilink control subsystem exists
wfPppMlStatsLineCnt	Current count of lines in the multilink bundle
wfPppMlStatsBundleSpd	Current total bandwidth of the multilink bundle
wfPppMlStatsMrru	Current Maximum Receive Reconstructed Unit (MRRU) in use for the multilink bundle
wfPppMlStatsEndptDisc	Current Endpoint Discriminator in use for the multilink bundle
wfPppMlStatsTxOctets	Number of octets transmitted by multilink
wfPppMlStatsTxPkts	Number of packets transmitted by multilink
wfPppMlStatsAvgTxListLen	Average number of packets received in the transient list by the Multilink Transmit gate
wfPppMlStatsRxOctets	Number of octets received without error
wfPppMlStatsRxPkts	Number of packets received by multilink
wfPppMlStatsReasmFails	Number of packet reassembly failures
wfPppMlStatsSeqNumberLost	Number of multilink packets considered to be lost on the wire

Table B-1. PPP Statistics *(continued)*

MIB object name	What it tells you
wfPppMlStatsSeqNumberArrivedLate	Number of multilink packets that arrive containing an old sequence number; that is, packets with a more current sequence number have already been sent up to NCP
wfPppMlStatsReSeqBufferCnt	Number of multilink packets currently stored in the ReSequencing buffer pool
wfPppMlStatsReSeqBufferMax	The maximum number of multilink packets stored in the ReSequencing buffer pool
wfPppMlStatsExceededBufferMax	The number of times a buffer needed to be stored by the Multilink Receive logic when the count of buffers stored, wfPppMlStatsReSeqBufferMax, was equal to the maximum allowable for this circuit,wfPppCircuitMaxBuffers
wfPppMlStatsLinkIdleEvents	The number of times the Multilink Receive logic detected a stored buffer received on a line what has been declared idle
wfPppMlStatsCalcPercent	Enable/disable calculating the percentage of multilink octets received on the line.

Index

A

Allow PAP Reject parameter 4-30
  default setting A-3
AppleTalk Control Protocol 1-3
AppleTalk Enable parameter 4-7
  default setting A-1
AppleTalk Routing Protocol parameter 4-12
  default setting A-2
authentication protocols
  CHAP 1-2, 1-7
  PAP 1-2, 1-7
  setting parameters 4-21, 4-28
  using with dial services 1-7

B

bandwidth-on-demand 1-2, 2-2
Bay Networks
  CompuServe forum xiii
  customer support xiii
  Home Page on World Wide Web xiv
  InfoFACTS service xiv
  publications, ordering xv
  Technical Response Center xiv
BNX software
  HSSI link quality monitoring 1-9
  IP Enable parameter 4-5
  prioritization mechanism 2-6
BOFL synchronous line parameter 2-8
Bridge Enable parameter 4-8
  default setting A-2
Bridge Ethernet parameter 4-12
  default setting A-2
Bridge FDDI parameter 4-13
  default setting A-2
Bridge Network Control Protocol (BNCP) 1-3
Bridge Token Ring parameter 4-13
  default setting A-2

C

CCP Enable parameter 4-9
  default setting A-2
Challenge Handshake Authentication Protocol (CHAP) 1-2, 1-7, 2-2
  setting parameters 4-21, 4-28
CHAP Local Name
  identification mechanism 2-2
Chap Local Name
  and Interface for Dialup Lines 4-15
  identification mechanism 1-2, 4-15
  used for authentication 1-2
Chap Local Name parameter 4-29
  default setting A-3
Chap Periodic Timer parameter 4-29
  default setting A-3
Chap Secret parameter 4-28
  default setting A-3
circuit statistics
  calculating and viewing 2-11
comparing multiline and PPP multilink 2-7
compatibility with previous versions 2-9
Compression Control Protocol (CCP) 4-9
compression, data 2-1

CompuServe, Bay Networks forum on xiii
Configure-ACK packet 1-5
Configure-NAK packet 1-5
  setting maximum number 4-20
Configure-Reject packet 1-5
Configure-Request packet 1-4
  setting maximum number 4-19
configuring PPP interfaces
  guidelines 2-1
congestion monitor 2-4
customer support. *See* getting help

D

data compression 2-1
  enabling on PPP interface 4-9
data link control protocols
  authentication 1-2, 1-7
  maximum receive unit 1-2
  quality protocol 1-2
datagram encapsulation 1-8
DECnet IV Enable parameter 4-7
  default setting A-1
DECnet Phase IV Control Protocol 1-3
defaults
  for interface parameters A-1
  for line parameters A-3
deleting PPP globally 4-30
dial backup 1-2, 2-2, 4-28
dial services 2-2
  identification mechanism 1-2, 1-7
  PPP support 2-2
dial-on-demand 1-2, 2-2, 4-28
  implementation notes 2-6
dial-up line
  PPP support 2-2

E

Echo-Reply Acceptable Loss parameter 4-19
  default setting A-3
editing parameters
  interface 4-2
  line 4-15
Enable (LCP) parameter 4-18
  default setting A-3
Enable PAP Fallback parameter 4-25
  default setting A-3
encapsulation 1-8

F

frame structure 1-8

G

getting help
  from a Bay Networks Technical Response Center xiv
  through CompuServe xiii
  through InfoFACTS service xiv
  through World Wide Web xiv

I

implementation notes
  dial-on-demand 2-6
Inbound Link Quality parameter 4-27
  default setting A-3
incompatibilities 2-9
InfoFACTS service xiv
interface initialization phases 1-4
Interface parameters 4-5
interface parameters, editing 4-2
IP Enable parameter 4-5
  default setting A-1
IP, enabling on a PPP interface 2-10

IPX Enable parameter 4-8
default setting A-1
IPX Network Number parameter 4-10
default setting A-2
IPX Remote Node Number parameter 4-11
default setting A-2
IPXCP 1-3

L

line parameters
synchronous 2-8
line parameters, editing 4-15
line statistics
calculating and viewing 2-11
Link Control Protocol (LCP)
definition 1-4
negotiations
Configure-Ack 1-5
Configure-NAK 1-5
Configure-Reject 1-5
Configure-Request 1-4
link establishment using PPP 1-4
link monitoring 1-9
setting parameters 4-26
link quality monitoring 1-9
Link Quality Protocol 1-2
Link Quality Protocol parameter 4-26
default setting A-3
link quality report 1-9
link routing using PPP 1-3
Local Authentication Protocol parameter 4-21
default setting A-3
Local PAP ID parameter 4-22
default setting A-3
Local PAP Password parameter 4-23
default setting A-3
LQM 1-9
LQR 1-9
LQR Reporting Period parameter 4-27
default setting A-3

M

Max A-2
Max Buffers parameter
default setting A-2
Max Configuration Failure Count parameter 4-20
default setting A-3
Max Configure-Requests parameter 4-19
default setting A-3
Max Links parameter
default setting A-2
Max Terminate-Requests parameter 4-20
default setting A-3
monitor, congestion 2-4
monitoring PPP links 1-9
multilink
configuring 2-6
multilink and multiline
comparison 2-7
Multilink Endpoint Discriminator 1-2

N

network connection
establishing 1-8
Network Control Protocol (NCP)
disabling 2-10
Network Control Protocols (NCPs)
disabling 2-10
network security 1-2, 1-7

O

OSI Enable parameter 4-6
default setting A-1
OSI Network Layer Control Protocol 1-3
Outbound Link Quality parameter 4-28
default setting A-3

P

PAP 1-2, 1-7, 2-2
  setting parameters 4-21
PAP ID
  and Interface for Dialup Lines 4-15
  identification mechanism 1-2, 2-2
  used for authentication 1-2
parameters
  default settings A-1–A-3
  interface
    AppleTalk Enable 4-7, A-1
    AppleTalk Routing Protocol 4-12, A-2
    Bridge Enable 4-8, A-2
    Bridge Ethernet 4-12, A-2
    Bridge FDDI 4-13, A-2
    Bridge Token Ring 4-13, A-2
    CCP Enable 4-9, A-2
    DECnet IV Enable 4-7, A-1
    editing 4-2
    IP Enable 4-5, A-1
    IPX Enable 4-8, A-1
    IPX Network Number 4-10, A-2
    IPX Remote Node Number 4-11, A-2
    Max Buffers A-2
    Max Link A-2
    OSI Enable 4-6, A-1
    PPP Mode A-2
    Remote AppleTalk Node 4-11, A-2
    Remote IP Address 4-10, A-2
    VINES Enable 4-9, A-2
    XNS Enable 4-6, A-1
  line 4-15
    Allow PAP Reject 4-30, A-3
    Chap Local Name 4-29, A-3
    Chap Periodic Timer 4-29, A-3
    Chap Secret 4-28, A-3
    Echo-Reply Acceptable Loss 4-19, A-3
    Enable (LCP) 4-18, A-3
    Enable PAP Fallback 4-25, A-3
    Inbound Link Quality 4-27, A-3
    Link Quality Protocol 4-26, A-3
    Local Authentication Protocol 4-21, A-3
    Local PAP ID 4-22, A-3
    Local PAP Password 4-23, A-3
    LQR Reporting Period 4-27, A-3
    Max Configuration Failure Count 4-20, A-3
    Max Configure-Requests 4-19, A-3
    Max Terminate-Requests 4-20, A-3
    Outbound Link Quality 4-28, A-3
    Peer Link Quality Report Timer 4-26, A-3
    Remote PAP ID 4-24, A-3
    Remote PAP Password 4-25, A-3
    Restart Timer in Seconds 4-18, A-3
    Seconds between Xmit of Echo-Request 4-18, A-3
  synchronous line 2-8
Password Authentication Protocol (PAP) 1-7, 2-2
  setting parameters 4-21
Peer Link Quality Report Timer parameter 4-26
  default setting A-3
Point-to-Point Protocol. *See* PPP
PPP
  deleting 4-30
  enabling 3-1
  implementation notes 2-1, 2-10
  Link Control Protocol (LCP) 1-4
  overview 1-1
  parameter default settings A-1–A-3
  statistics B-1
PPP Interface Lists window 4-5
PPP Interface parameters 4-5
PPP Line parameters 4-15
PPP Mode parameter
  default setting A-2
prioritization
  BNX software 2-6
  protocol 2-6
Promiscuous synchronous line parameter 2-8
protocol prioritization 2-6
protocols
  data link control options 1-2
  network 1-3

Q

quality monitoring for link(s) 1-9

R

receive percentages
  calculating and viewing 2-11
Remote AppleTalk Node parameter 4-11
  default setting A-2
Remote IP Address parameter 4-10
  default setting A-2
Remote PAP ID parameter 4-24
  default setting A-3
Remote PAP Password parameter 4-25
  default setting A-3
Restart Timer in Seconds parameter 4-18
  default setting A-3
RFCs relevant to PPP 2-9
routing over a PPP link 1-3

S

Seconds between Xmit of Echo-Request parameter 4-18
  default setting A-3
Service synchronous line parameter 2-8
software incompatibilities 2-9
source-routing over Token Ring networks
  incompatibilities 2-9
statistics B-1
  calculating and viewing 2-11
switched line
  PPP support 2-2
synchronous line parameters 2-8

T

Technician Interface
  statistics B-1
Token Ring networks
  incompatibilities 2-9

V

Versions 5.x, 7.x, 8.x, and 9.x router software 2-9
VINES Enable parameter 4-9
  default setting A-2
VINES Network Control Protocol 1-3

W

WAN Protocol synchronous line parameter 2-8
World Wide Web, Bay Networks Home Page on xiv

X

Xerox Network System Control Protocol (XNSCP) 1-3
XNS Enable parameter 4-6
  default setting A-1